Forcepoint DSPM

Forcepoint

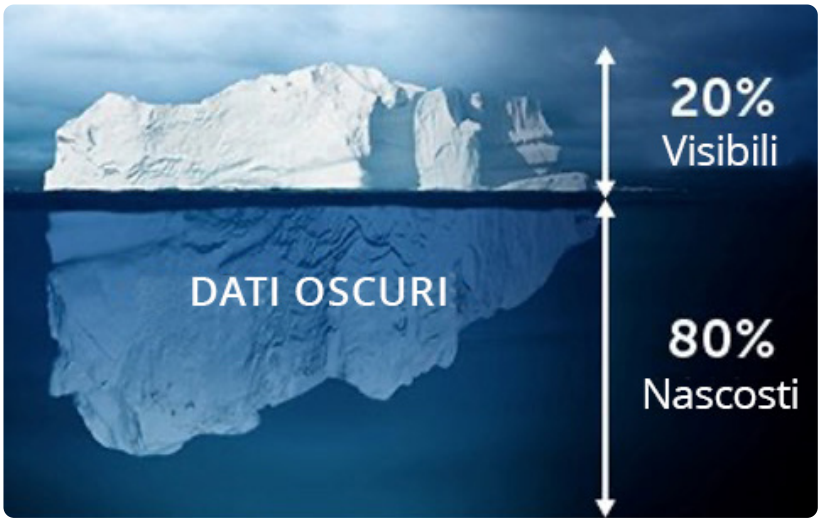
Brochure

forcepoint.com/it

Trasformazione dell'IA: il prossimo step della trasformazione digitale

In questa nuova era i tuoi dati sono al sicuro?

La maggior parte delle organizzazioni che hanno implementato processo di trasformazione digitale si sta preparando per il passo successivo: la trasformazione dell'IA. Questa nuova era dell'IA è guidata dai numerosi vantaggi offerti dalle applicazioni GenAI come ChatGPT, Copilot, Gemini e altre ancora. Grazie a tali esperienze di trasformazione digitale, le organizzazioni hanno imparato che la sicurezza dei dati deve essere una priorità assoluta. Tuttavia, per molti, i dati oggi sono come una sorta di gigantesco iceberg, dove la maggior parte delle informazioni è nascosta sotto la superficie dell'acqua. Spesso definiti come "dati oscuri" o "dati ombra", rimangono invisibili e sconosciuti, eppure contengono una notevole quantità di informazioni sensibili per le quali le organizzazioni hanno una responsabilità diretta. In questo momento, le organizzazioni stanno cercando di capire come consentire agli utenti di sfruttare in modo sicuro le applicazioni GenAI per migliorare la produttività e l'efficienza, garantendo al contempo che i dati sensibili rimangano al sicuro.



DSPM (Data Security Posture Management) offre un approccio completo per proteggere le informazioni da accessi non autorizzati, diffusione, alterazione o distruzione dei dati. A differenza di altri tipi di metodi di sicurezza dei dati che si concentrano sui sistemi e sui dispositivi, DSPM si concentra sulla totalità dei dati di un'organizzazione, strutturati o non strutturati, che si tratti di proprietà intellettuale o dati regolamentati, nel cloud o sulle reti private, garantendo la conformità e mitigando il rischio di violazioni dei dati.

Secondo IDC, l'80% dei dati globali non sono strutturati, mentre il 90% di tali dati non sono stati analizzati, vengono anche chiamati "dati oscuri".[1]

Il 94% delle organizzazioni archivia i dati in più ambienti cloud.[2]

Equifax ha dovuto risarcire 1,4 miliardi di dollari a seguito di una violazione[3] dei dati aggravata dall'accesso di hacker a un drive condiviso contenente più copie di nomi utente e password dei dipendenti. L'azienda non aveva strumenti per rilevare e individuare i file ridondanti e obsoleti.

1 The Unseen Data Conundrum, Forbes, febbraio 2022

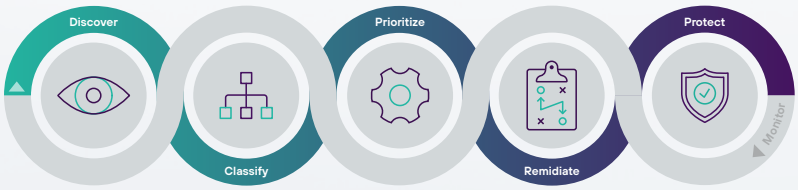
2 Dark Data: The Cloud's Unknown Security and Privacy Risk, Forbes, giugno 2023

3 Equifax agrees $1.38bn data breach lawsuit settlement, Finextra, gennaio 2020

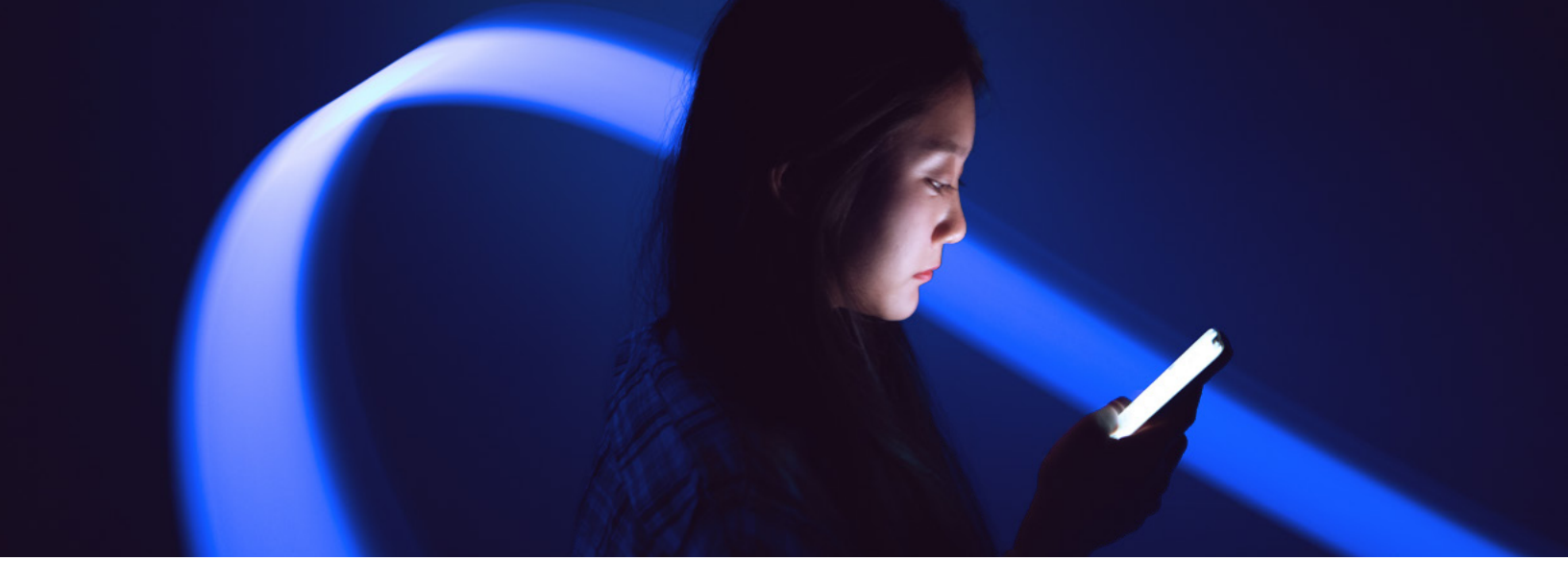
Cosa fa DSPM?

- **Percorso di trasformazione dell'IA:** libera il potenziale dell'IA con Forcepoint DSPM, salvaguardando i dati ovunque grazie alla nostra avanzata tecnologia AI Mesh. Con la visibilità e la risoluzione centralizzata da Forcepoint DSPM e i controlli di blocco in tempo reale da Forcepoint DLP, proteggiamo le tue informazioni sensibili attraverso i canali chiave, tra cui le applicazioni dell'IA generativa come ChatGPT, Copilot, Gemini e molti altri, potenziando l'innovazione audace e aumentando la produttività e riducendo il rischio.
- **Identificazione dei dati sensibili:** DSPM aiuta le organizzazioni a identificare i dati sensibili attraverso più ambienti e servizi cloud e le sedi on-prem, inclusi i dati strutturati e non strutturati. Ciò include la comprensione di dove risiedono i dati sensibili, come si accede e chi ha le autorizzazioni per interagire con essi.
- **Valuta la vulnerabilità e il rischio:** DSPM valuta la vulnerabilità dei dati sensibili alle minacce alla sicurezza e il rischio di mancata conformità alla normativa. Analizzando la posizione di sicurezza dei dati, le organizzazioni possono affrontare proattivamente i potenziali rischi.
- **Si concentra sui dati alla fonte:** a differenza di altri strumenti di sicurezza dei dati che proteggono principalmente dispositivi, sistemi e applicazioni, DSPM si concentra direttamente sulla protezione della totalità dei dati di un'organizzazione. Mira a prevenire le violazioni dei dati e a garantire la conformità proteggendo i dati al centro.
- **Rimedia i dati oscuri e i dati ROT:** DSPM rimedia direttamente i dati oscuri (dati attualmente non visualizzati o non utilizzati nei normali processi aziendali). Analogamente, DSPM è in grado di rimediare i dati ROT (dati ridondanti, obsoleti e banali), i quali solitamente proliferano nelle organizzazioni man mano che si accumulano i dati conservati per varie ragioni, nella convizione che ciò contribuisca alla conformità. In realtà, crea un rischio ancora maggiore per i dati e DSPM aiuta a gestire tale rischio.
- **Rimedia i dati con autorizzazioni/esposizione eccessive:** a causa del modo in cui i dati proliferano mediante la copia e la modifica di nuove versioni dei dati, spesso i dati possono estendersi a utenti, gruppi e persino all'intera organizzazione. DSPM aiuta a far rispettare il concetto di Zero Trust del "principio del privilegio minimo", che riduce drasticamente i dati con autorizzazioni eccessive al fine di prevenire le violazioni dei dati.
- **Ambienti multi-cloud e cloud ibridi:** con la crescente adozione di ambienti multi-cloud e cloud ibridi, il rischio di violazioni dei dati aumenta drasticamente. DSPM offre visibilità e controllo sui dati sensibili nei diversi ambienti di elaborazione oltre alle sedi locali.
- **Monitoraggio continuo del rischio:** il componente aggiuntivo di Forcepoint Data Detection and Response (DDR) consente a Forcepoint DSPM di rilevare e porre rimedio ai nuovi rischi per i dati nel momento in cui si verificano. Non è necessario attendere la prossima scansione DSPM completa: identifica dinamicamente i rischi per la posizione di sicurezza dei dati per porvi rimedio.

Forcepoint DSPM è progettato per le organizzazioni moderne che hanno bisogno di visibilità e controllo sui dati sensibili. Fornisce visibilità in vari ambienti cloud e server per prevenire le violazioni di dati e ridurre il rischio di mancata conformità rispetto alle normative sulla privacy. Forcepoint offre visibilità e controllo lungo l'intero ciclo di vita dei dati, proteggendo i dati ovunque, combinando il **rilevamento proattivo del rischio dei dati** (DSPM) con **controlli attivi sul modo in cui questi vengono utilizzati** (DLP) e **adattandosi continuamente alle azioni di ciascun utente** (Risk-Adaptive Protection). Ottieni la scoperta dinamica del rischio dei dati con il monitoraggio continuo (Forcepoint DDR) per prevenire le violazioni dei dati e proteggere la tua sicurezza dei dati.



Discovery, classificazione e orchestrazione basati sull'IA



Unisci visibilità e controllo sul panorama dei tuoi dati con Forcepoint DSPM

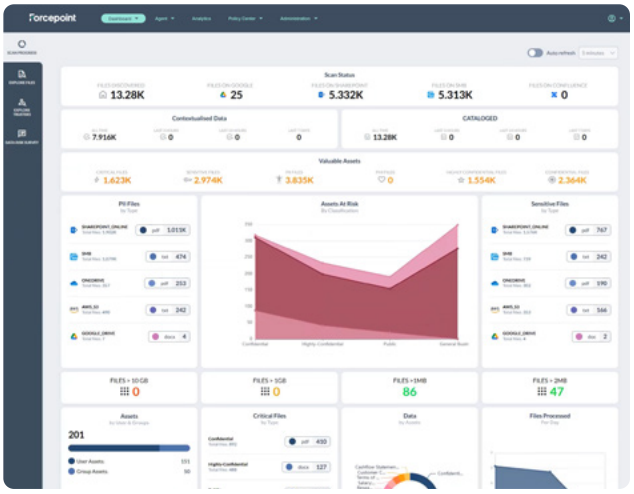
Gestire e proteggere i dati della tua organizzazione non è mai stato così complesso. Forcepoint DSPM offre una soluzione potente per ottenere visibilità e controllo completi sui tuoi dati, indipendentemente da dove si trovano. Con velocità di rilevamento e funzionalità avanzate di classificazione dei dati AI Mesh, Forcepoint DSPM ti consente di prendere decisioni informate sulla tua posizione di sicurezza dei dati e di affrontare in modo proattivo i potenziali rischi.

Tra i principali vantaggi di Forcepoint DSPM vi sono:

Scoperta rapida e completa: su più cloud e on-prem, Forcepoint DSPM è in grado di scansionare rapidamente file e database. i Spesso le organizzazioni sono responsabili di molti terabyte di dati, alcune persino petabyte, fino ad arrivare alle più grandi che possono trovarsi ad avere anche esabyte di dati. Grazie al rilevamento ad alte prestazioni, Forcepoint consente alle organizzazioni di visualizzare rapidamente le informazioni in volumi di dati enormi, incluso ChatGPT Enterprise. A differenza di altri fornitori di soluzioni DSPM, Forcepoint non addebita costi per le operazioni di rilevamento e i clienti possono eseguirle tutte le volte che desiderano, senza costi aggiuntivi.

Accuratezza dei dati grazie alla tecnologia "Rete IA": Forcepoint DSPM rileva i dati attraverso fonti cloud e di rete e li classifica automaticamente utilizzando un avanzato motore di classificazione IA. "Rete IA" di Forcepoint DSPM consente alle organizzazioni di ottenere una precisione di classificazione dei dati di alto livello. La sua architettura IA in rete, che sfrutta un modello SLM GenAI, oltre che dati e componenti IA avanzati, rileva in modo efficiente il contesto dal testo non strutturato. Personalizzabile ed efficiente, garantisce una classificazione rapida e accurata senza una formazione approfondita, migliorando il grado di fiducia e conformità. Grazie alla sua elevata precisione, ha consentito alle organizzazioni che hanno riscontrato problemi con altri metodi di classificazione diffusi di ridurre drasticamente i falsi positivi/negativi, riuscendo a proteggere la proprietà intellettuale e ottenendo un grande risparmio in termini di tempo e risorse.

Visibilità su tutto il panorama dei dati: Forcepoint DSPM consente di ispezionare le autorizzazioni per tutti i file e gli utenti. Gli amministratori dei dati possono visualizzare chi può accedere a un file o a file condivisi in tutta l'organizzazione. Con un solo clic è possibile visualizzare immediatamente le autorizzazioni per tutti i file scansionati. Forcepoint DSPM fornisce una dashboard con dettagli approfonditi che offrono una visione a volo d'uccello sui dati oscuri e forniscono una valutazione panoramica del rischio dei dati per aiutarti a comprendere le aree a più alto rischio per i dati.



Orchestrazione del flusso di lavoro: definisci facilmente la proprietà e la responsabilità per diversi set di dati per facilitare l'allineamento tra i vari stakeholder. Ciò consente flussi di lavoro più efficienti sulle azioni eseguite su ciascuna fonte di dati e risorsa. Una riparazione effettiva richiede un ampio coinvolgimento e una collaborazione oltre all'organizzazione della sicurezza per il gruppo CDO/Governance o Risk & Compliance (GRC) nonché funzioni come marketing, finanza, DevOps e molto altro. Forcepoint DSPM considera la protezione dei dati non solo come un problema di sicurezza, ma come una priorità del business.

Forcepoint DDR: un potente aggiunta a Forcepoint DSPM, rappresenta una soluzione chiave per affrontare le violazioni dei dati. Fornisce il rilevamento continuo della minaccia e una visibilità avanzata del rischio dei dati, garantendo che le organizzazioni possano vedere efficacemente le modifiche ai dati che probabilmente portano a violazioni dei dati man mano che si verificano. Sfruttando risposte basate sull'IA, Forcepoint DDR offre una precisa neutralizzazione delle minacce, aiutando le organizzazioni a mantenere solide misure di sicurezza. La sua ampia visibilità su cloud ed endpoint, combinata con il tracciamento della provenienza dei dati, lo rende uno strumento essenziale per proteggere le informazioni sensibili, ridurre le perdite finanziarie e mantenere la fiducia dei clienti.

Non lasciare che i dati a rischio paralizzino la tua azienda. Forcepoint può aiutarti

Nell'era digitale di oggi, i dati sono un patrimonio prezioso per le organizzazioni, ma possono anche diventare un onere, se non vengono gestiti correttamente. Forcepoint DSPM offre un approccio proattivo per proteggere i dati sensibili, mitigare i rischi di violazioni e garantire la conformità alle normative. Implementando Forcepoint DSPM, puoi ottenere una visibilità completa sul tuo panorama dei dati, individuare e risolvere le vulnerabilità e proteggere in modo proattivo la tua organizzazione dagli eventuali danni finanziari e reputazionali causati da violazioni dei dati e dalla mancata conformità alle normative, proteggendo al contempo i tuoi dati nelle applicazioni GenAI. Prendi il controllo della tua posizione di sicurezza dei dati oggi stesso. Scopri come la soluzione DSPM può proteggere le tue preziose informazioni. Vai su www.forcepoint.com/it/dspm per richiedere una demo oppure iscriviti per una valutazione gratuita: una persona del nostro team di sicurezza eseguirà una prova per scoprire qual è l'attuale grado di rischio dei tuoi dati.

Forcepoint

forcepoint.com/contact

Su Forcepoint

Forcepoint semplifica la sicurezza per aziende e governi di tutto il mondo. La sua piattaforma all-in-one e nativa cloud facilita l'adozione della Zero Trust e impedisce i furti o le perdite di dati sensibili e proprietà intellettuale indipendentemente da dove lavorano le persone. Con sede a Austin, Texas, Forcepoint crea ambienti sicuri e affidabili per i clienti e i loro dipendenti in oltre 150 paesi. Contatta Forcepoint su www.forcepoint.com, Twitter e LinkedIn.

[FP-DSPM-Brochure-IT] 30Sept2025